UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,773	03/09/2004	Mark Ammar Rayes	50325-0865	4164

29989 7590 05/21/2007

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
SHAIFER HARRIMAN, DANT B	

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
05/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/797,773	RAYES ET AL.	
	Examiner	Art Unit	
	Dant B. Shaifer - Harriman	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09/2/04*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/28/05,12/06/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claim(s) 21 – 23 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim 21 –23. See MPEP § 608.01(n). Accordingly, the claims 21 –23 have not been further treated on the merits.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claim(s) 19 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Please see In re Hyatt 708 F.2d 712, 714-715, 218 USPQ 195, 197 (Fed. Cir. 1983), which discusses the error regarding single means plus function claims.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim(s) 19, 22, 25 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claim(s) 1-2 & 9-14 & 17 – 26 are rejected under 35 U.S.C. 102(b) as being taught by Freund (US Patent # 5987611).

Freund teaches:

- Claim #1. A method, comprising the computer-implemented steps of: determining a user identifier associated with a network device that has caused a security event in a network, (Col 12. Lines 54-65, the examiner notes that a access management application or firewall or filter tracks data packet flow by the source/destination address);

- causing the network device to receive a network address that is selected from a subset of addresses within a specified pool associated with suspected

malicious network users (Col. 12, Lines 66 – 67 & Col. 13, lines 1-22), the examiner notes that a access management application or firewall or packet filter will have a data base or table that is predefined with what particular malicious addresses to look for with particular network users.)

- configuring one or more security restrictions with respect to the selected network address(Col 12. Lines 54-65, the examiner notes that a access management application or firewall or filter will inherently have rules, policy, security restrictions associated with particular legal operations that the firewall monitors data packet traffic with).

Claim #2 A method as recited in Claim 1, further comprising the steps of:

- receiving information identifying the security event in the network (Col 12. Lines 54-65, the examiner notes that a access management application or packet filter or firewall or router which contains firewall, will have the means of reading each data packet by reading the source/destination address, which is inherently allows the firewall or router to identify the network device and associated network device information and what illegal operation it performed.);

- correlating the security event information with network user information to result in determining the user identifier associated with the network device (Col 12. Lines 54-65, the examiner notes that a access management

application or packet filter or firewall or router which contains firewall, will have the means of reading each data packet by reading the source/destination address, which is inherently allows the firewall or router to identify the network device and associated network device information and what illegal operation it performed.

The examiner further rejects claim 21, 22, 23 based on the reasoning and logic that claim 2 was rejected on. Claims 21, 22, 23 are rejected based on the fact that the computer-readable medium, and apparatus are merely the implementation of the method and when executed will produce the same results as the method (Col. 28, lines 14 – 32, the examiner notes that the local storage medium can be ether a apparatus or computer readable medium, the supervisor utilizes the storage medium for policy enforcement).

Claim #9.A method as recited in Claim 1, wherein the step of configuring security restrictions comprises the steps of modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the selected network address, (Col 12. Lines 54-65, the examiner notes that a access management application or firewall or packet filter will teach or can be configured to have a rule database or policy manager that has predefined network addresses that it trust and doesn't, and will allow certain data packet flows through the firewall without analyzing the data packet flow associated with the network address or

network device.)

Claim #10. A method as recited in Claim 1, wherein the step of configuring security restrictions comprises the steps of modifying a media access control (MAC) ACL associated with a port that is coupled to the network device to permit entry of traffic only for a MAC address that is bound to the selected network address, (Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that a access management application or firewall or packet filter will have a predefined URL or address lists that consist of network addresses that the access management application or firewall or packet filter will/will not allow data or communication with the user or network device through particular ports of the network device.

Claim #11. A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, and if so, providing information about the security event or malicious act to a security decision controller, (Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that the access management application or firewall or packet filter has a set of rules, that are predefined and are used to look for malicious activity, hence the access management application decides whether or not incoming packet data flow matches the predefined rules list, i. e. compare whether or not a rule has been broken.)

Claim #12. A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, and if not, removing the user from the

elevated risk group, (Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that the access management application or firewall or packet filter has a set of rules, that are predefined and are used to look for malicious activity, once this malicious activity has been detected, the user or network device or devices could be log in as a malicious user among other malicious user, and if the access management application determines that a rule hasn't been broken, then the user will be allowed or release to have access to various applications and will also be removed from the log as a malicious user.)

Claim #13. A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, wherein a legal user action in the network is not determined to be a malicious act if the user is associated with a trusted customer of a network service provider, (Col. 21, lines 48-56, the examiner notes that ISP's or internet service providers will have a firewall or packet filter or access management that can determine whether malicious act is occurring, the access management or firewall or packet filter per se will be able to tell if user or network device is associated with a trusted internet service provider, based on the data packets source/destination address that is associated with the user request to access the network.)

Claim #14. A method, comprising the computer-implemented steps of:

- receiving information identifying a security event in a network(Col 12. Lines 54-65, the examiner notes that a access management application or packet filter or firewall or router which contains firewall, will have the means of reading each data packet by reading the source/destination

address, which is inherently allows the firewall or router to identify the network device and associated network device information and what illegal operation it performed.) ;

- correlating the security event information with network user information to result in determining a network user associated with the network device(Col 12. Lines 54-65, the examiner notes that a access management application or packet filter or firewall or router which contains firewall, will have the means of reading each data packet by reading the source/destination address, which is inherently allows the firewall or router to identify the network device and associated network device information and what illegal operation it performed.).

- placing the user in an elevated risk security group(Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that the access management application or firewall or packet filter has a set of rules, that are predefined and are used to look for malicious activity, once this malicious activity has been detected, the user or network device or devices could be log (i.e. elevated risk user group) in as a malicious user among other malicious user, and if the access management application determines that a rule hasn't been broken, then the user will be allowed or release to have access to various applications and will also be removed from the log (i.e. elevated risk user group) as a malicious user.)

- configuring one or more security restrictions with respect to the selected network address(Col 12. Lines 54-65, the examiner notes that a access management application or firewall or filter will inherently have rules, policy, security restrictions associated with particular legal operations that the firewall monitors data packet traffic with.);

- determining whether a malicious act caused the security event(Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that the access management application or firewall or packet filter has a set of rules, that are predefined and are used to look for malicious activity, once this malicious activity has been detected, the user or network device or devices could be log (i.e. elevated risk user group) in as a malicious user among other malicious user, and if the access management application determines that a rule hasn't been broken, then the user will be allowed or release to have access to various applications and will also be removed from the log (i.e. elevated risk user group) as a malicious user.);

- if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller (Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that a access management application or firewall or packet filter will have a predefined URL or address lists that consist of network addresses that the access management application will/will

not allow data or communication with the user or network device.);

- if a malicious act did not cause the security event, then removing the user from the elevated risk group (Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that the access management application or firewall or packet filter has a set of rules, that are predefined and are used to look for malicious activity, once this malicious activity has been detected, the user or network device or devices could be log (i.e. elevated risk user group) in as a malicious user among other malicious user, and if the access management application determines that a rule hasn't been broken, then the user will be allowed or release to have access to various applications and will also be removed from the log (i.e. elevated risk user group) as a malicious user.)

The examiner further rejects claim 24, 25 based on the reasoning and logic that claim 14 were rejected on. Claims 24, 25 are rejected based on the fact that the computer-readable medium, and apparatus are merely the implementation of the method and when executed will produce the same results as the method (Col. 28, lines 14 – 32, the examiner notes that the local storage medium can be ether a apparatus or computer readable medium, the supervisor utilizes the storage medium for policy enforcement).

Claim #17. A method as recited in Claim 14, wherein the step of configuring one or more security restrictions comprises the steps of:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the selected network address(Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that a access management application or firewall or packet filter will have a predefined URL or address lists that consist of network addresses that the access management application will/will not allow data or communication with the user or network device.)

- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the selected network address(Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that a access management application or firewall or packet filter will have a predefined URL or address lists that consist of network addresses that the access management application will/will not allow data or communication with the user or network device.)

Claim #18. A computer-readable medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

- determining a user identifier associated with a network device that has caused a security event in a network (Col. 12, lines 54-65, the examiner notes that a access management application or firewall or filter tracks data packet flow by the

source/destination address, the examiner further notes that the computer – readable medium is merely the implementation of the method, and will thus produce the same result as the method);

- causing the network device to receive a network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users(Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that a access management application or firewall or packet filter will have a data base or table that is predefined with what particular malicious addresses to look for with particular network users; the examiner further notes that the computer – readable medium is merely the implementation of the method, and will thus produce the same result as the method.)

- configuring one or more security restrictions with respect to the selected network address(Col. 12, lines 54-65, the examiner notes that a access management application or firewall or filter will inherently have rules, policy, security restrictions associated with particular legal operations that the firewall monitors data packet traffic with; the examiner further notes that the computer – readable medium is merely the implementation of the method, and will thus produce the same result as the method).

Claim #19. An apparatus, comprising:

means for determining a user identifier associated with a network device that has

caused a security event in a network (Col. 12, lines 54-65, the examiner notes that a access management application or firewall or filter tracks data packet flow by the source/destination address; the examiner further notes that the apparatus is merely the implementation of the method, and thus will produce the same result as the method when executed.)

- means for causing the network device to receive a network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users(Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that a access management application or firewall or packet filter will have a data base or table that is predefined with what particular malicious addresses to look for with particular network users; the examiner further notes that the apparatus is merely the implementation of the method, and thus will produce the same result as the method when executed.)

- means for configuring one or more security restrictions with respect to the selected network address(Col. 12, lines 54-65, the examiner notes that a access management application or firewall or filter will inherently have rules, policy, security restrictions associated with particular legal operations that the firewall monitors data packet traffic with; ; the examiner further notes that the apparatus is merely the implementation of the method, and thus will produce the same result as the method when

executed.)

Claim #20. An apparatus, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom (Col. 12, lines 54-65, the examiner notes that a access management application or firewall will inherently have a network interface or graphical user interface, for the administer of the firewall to configure the firewall to his or her security needs; the examiner further notes that the apparatus is merely the implementation of the method, and thus will produce the same result as the method when executed.)

- a processor (Col. 12, lines 54-65, the examiner notes that a access management application or firewall with packet filter, inherently is a processor, meaning when a data packet flow (i.e. an e-mail) is sent to a recipient, the email message is copped up into data packets, that must be processed (i.e. firewall looking for viruses or illegal operations associated with the data packets) through the recipients firewall before the recipient can view the e-mail safely; the examiner further notes that the apparatus is merely the implementation of the method, and thus will produce the same result as the method when executed.)

- one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of (Col. 12, lines 54-65: the examiner notes that a access management application or firewall or packet filter will by inherency have a stored sequences instructions or what types of illegal operations or viruses to look for in the data packet flow into and out of the firewall; the examiner further notes that the apparatus is merely the implementation of the method, and thus will produce the same result as the method when executed.)

- determining a user identifier associated with a network device that has caused a security event in a network (Col. 12, lines 54-65, the examiner notes that a access management application or firewall or filter tracks data packet flow by the source/destination address; the examiner further notes that the apparatus is merely the implementation of the method, and thus will produce the same result as the method when executed.

- causing the network device to receive a network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users (Col. 12, Lines 66 – 67 & Col. 13, lines 1-22, the examiner notes that a access management application or firewall or packet filter will have a data base or table that is predefined with what particular malicious addresses to look for with particular network users; the examiner further notes that the apparatus is merely the

implementation of the method, and thus will produce the same result as the method when executed.

- configuring one or more security restrictions with respect to the selected network address (Col. 12, lines 54-65, the examiner notes that a access management application or firewall or filter will inherently have rules, policy, security restrictions associated with particular legal operations that the firewall monitors data packet traffic with; the examiner further notes that the apparatus is merely the implementation of the method, and thus will produce the same result as the method when executed.)

Claim #26. An apparatus, comprising:

- a network interface that is coupled to a data network for receiving one or more packet flows therefrom (Col. 12, lines 54-65:, the examiner notes that a access management application or firewall or filter will inherently have rules, policy, security restrictions associated with particular legal operations that the firewall monitors data packet traffic with; ; the examiner further notes that the apparatus is merely the implementation of the method, and thus will produce the same result as the method when executed.);

- a processor (Col. 12, lines 54-65, the examiner notes that a access management application or firewall with packet filter, inherently is a processor, meaning when a data packet flow (i.e. an e-mail) is sent to a recipient, the email message is copped up into data packets, that must be processed (i.e. firewall looking for viruses or illegal operations associated with the data packets) through the recipients firewall before the recipient can view the e-mail safely; the examiner further notes that the apparatus is merely the implementation of the method, and thus will produce the same result as the method when executed.) and

- one or more stored sequences of instructions which, when executed by the processor,

  cause the processor to carry out the steps as recited in any of Claims 14, 15, 16, or 17.(Col. 12, lines 54-65: the examiner notes that a access management application or firewall or packet filter will by inherency have a stored sequences instructions or what types of illegal operations or viruses to look for in the data packet flow into and out of the firewall; the examiner further notes that the apparatus is merely the implementation of the method, and thus will produce the same result as the method when executed.)

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim #3,4,5,6,7,8, 15, 16 is rejected under 35 USC 103(a) as being obvious over Freund (US Patent # 5987611) in view of (Hanson et al.(US PGPub # 2002/20098840)).

Freund discloses user identifier of network device, causing a network device to receive a network address from pool of addresses, security restrictions associated with the selected network address; Col. 12 , lines 45 -53, Col. 12, lines 54-65, and Col. 12, Lines 66 – 67 & Col. 13, lines 1-22.

Freund does not appear to explicitly disclose network device uses DHCP to obtain a network address, the network device receives a network address that comprises resetting a port that is coupled to the network device to prompt the user to command the network device to request a new network address using DHCP.

However, Hanson discloses network device obtains a network address by DHCP; Paragraph: 0304

Freund and Hanson are analogous art because they are from the "same field of endeavor," and managing device access on the internet in a computing environment.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Freund and Hanson before him or her, to modify the client filter and access management application of Freund to include the network device to retrieve a alternative network address by DHCP of Hanson because (it would allow the network device to obtain a new network address from a pool of addresses that is associated with malicious users, and allow network security to analyze it separately from the rest of the network traffic, without disrupting or slowing the network by using up all of the system resources.

The suggestion/motivation for doing so would have been (it would allow the network device to obtain a network address so the network security or filter or firewall would be able to monitor the suspected malicious, with out using up system resources and slowing down the performance of the network, Paragraph: 0457.)

Therefore, it would have been obvious to combine Freund with Hanson to obtain the invention as specified in the instant claims(s).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dant B. Shaifer - Harriman whose telephone number is 571-272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DSH 5/16/07

JOSEPH DEL SOLE
SUPERVISORY PATENT EXAMINER
5/10/07